In-Vehicular Mobile Router: Challenges and Approaches[1]

Extended Abstract for MMC 2003

Michael Wolf[*], Alex Petrescu[♦], Hong-Yon Lach[♦], Huamin Xu[♣], Markus Pilz[♣], Matthias Frank[♣], Miklós Aurél Rónai[●]

[*]DaimlerChrysler AG, Telematics Research, P.O.Box 2360, 89013 Ulm, Germany
[♦]Motorola Labs, Espace Technologique de St Aubin, 91193 Gif-sur-Yvette, France
[♣]University of Bonn, Institute of Computer Science IV, Römerstraße 164, 53117 Bonn, Germany
[●]Ericsson Research, Traffic and Network Performance Laboratory, P.O. Box 3, 1300 Budapest, Hungary

michael.m.wolf@daimlerchrysler.com
{petrescu,lach}@crm.mot.com
{pilz,xu,matthew}@cs.uni-bonn.de
Miklos.Ronai@eth.ericsson.se

Introduction

The European research project OverDRiVE aims at, among other goals, developing IPv6 protocols to support mobility of hosts, as well as of networks, that are deployed in vehicular environments. The scenarios considered in OverDRiVE envision that future vehicular environments in trains, ships or cars provide on-line information to the driver and passengers; moreover, in some cases, provide even access to the vehicular communication infrastructure from the outside world. All electronic devices and appliances deployed in a vehicle (laptop PCs, screens, engine computers and sensors) are connected together with IPv6 protocols, and connected to the IPv6 Internet.

In the following, we present the relevant OverDRiVE scenario that exposes the need for IPv6 **mobile networks**; then the next section presents the challenges and the technical approaches for mobile routers deployed in mobile networks; finally, we give an outlook to the content of the full paper and also identify future work.

Intra Vehicular Area Network (IVAN) Description and the OverDRiVE Scenario

In-car vehicular environments are more and more subject to introduction of highly sophisticated electronic equipment, ranging from simple sensor/actuator devices, to 1-chip embedded computers, to various types of LCD and TFT screens, to wireless networking equipment, and to full general purpose Personal Computers, laptops and routers. In-car networks are complex systems that offer engine-control services, driving assistance services and Internet access for drivers and passengers. Traditionally, separate "small networks" offer these type of services; for example Internet access is handled via the GSM/GPRS capable phone; another example is a DVB-T system that displays DVB-T channels to the build-in display device. A potentially highly interesting application, which can result from mixing the two technologies, is to receive personalized data via GSM/GPRS whereas more general information can be easily transmitted and broadcasted using the data transmission capabilities of the emerging DVB-T system. Another example is for the engine-control system to provide information to the car manufacturer's surveillance system at the technical center, that might issue an invitation for checkup, via the Internet, or even more sophisticated, allowing for remote software download (remote flash) via public radio access systems to car internal control units. These kinds of emerging applications are made possible by using open standards such as TCP/IP for networking.

A typical car network that is considered in OverDRiVE is connected to the Internet via a DVB-T system, via a GPRS/UMTS device and via WLAN interfaces. Moreover, the in-car network has various forms of WLAN components (802.11b) or Bluetooth. Wired car network technologies such as MOST and CAN/Flexray are perfect candidates for types of services involving high reliability and real time response times. It is clear though that TCP/IP protocols are not designed to support such characteristics as high-level of reliability. This is why, in OverDRiVE, these types of networks are being considered as layer 2 technologies that must support in a simple manner the IP protocols as layer 3 and above.

[1] This work is performed in the framework of the IST project IST-2001-35125 OverDRiVE, which is partly funded by the European Union.

An Intra Vehicular Area Network (IVAN) network is considering all the above aspects of in-car networks as well as the connection to the Internet. Moreover, it encompasses protocols to support continuous IP sessions for one of several hosts, based on Mobile IP. From a security standpoint, the IVAN network supports secure access into and out of the car.

Challenges and Approaches in Using IPv6 for Moving Vehicles

One challenge to bring IPv6 to vehicles is how to support mobility for multiple nodes that are moving as a whole. As described in the scenarios (section above), mobility is not only seen as the ability for a node to change its link point of attachment but also to provide reachability of a node and transparency for protocol layers above IPv6 (seamless handover). This ensures a migration path from well-known applications, e.g. web browsing, which relay on TCP or UDP as transport protocols, towards new mobile information services. An approach that solves the mobility for hosts is Mobile IPv6. Although standardization of Mobile IPv6 was still pending at the time of writing, it is mature enough to provide a basis for further investigations. The extension of Mobile IPv6 takes into account situations where the host mobility leads to waste of network resources. Using standard MobileIP the mobile nodes (MN) report the changes of their point of attachment to the network infrastructure by sending binding update messages (BU) to their home agents (HA) and correspondent nodes (CN). That would mean that in a scenario where MNs visit a mobile network every MN would have to care about its own mobility bindings resulting in binding update (BU) storm (through the scarce radio resource) whenever the mobile router changes its point of attachment. The same holds for inter-vehicular mobility (e.g. moving with a MN from one train wagon to another one). These kinds of inefficiencies should be avoided, and one approach is for the mobile router or the network infrastructure to act on behalf of mobile nodes for all activities concerning mobility.

In a simple mobile network scenario only Local Fixed Nodes (LFNs) are attached to mobile network link through a Mobile Router (MR). The mobile network moves homogeneously (as one unit) and only the Mobile Router changes its point of attachment as well as its Care-of Address, all mobility aspects being invisible to the Local Fixed Nodes. In a car environment, this can translate into having one MR connecting to Internet offered by GPRS/UMTS and all the passengers' laptops as LFNs. Composed, or nested, mobile networks contain several slices of networks that dynamically attach to each other in a more or less hierarchical manner. This can translate into for example a passenger carrying a Personal Area Network (PAN) that walks into the car where another mobile network is deployed.

Vehicular environments, especially in public transport branches, allow mobile users to attach to the mobile network most likely via wireless technologies. The deployment of security protocols and mechanisms in such an environment paves the way to grant access rights to individual users and enable charging for services, e.g. multimedia applications. An additional paper submitted to the MMC 2003 explicitly addresses the security issues involved in the described scenarios.

Common Approach for Network Mobility

In the full paper we will discuss the issues regarding mobile networks. We will describe several design options and possible solutions for instance to avoid the described BU storms. We will present in detail the integration of the mobile networks IPv6 protocol based on a bi-directional tunnel between MR and HA (Home Agent). Keywords are the scheme of prefix-scope binding updates and discussions regarding the pros and cons of several other approaches like dynamic routing protocols.

Conclusions

In conclusion, this paper presents the OverDRiVE aspects related to IP-level protocols for seamless Internet connectivity in a mobile network environment. The work has strong influence on work done in IETF NEMO (NEtwork MObility) group. Future work identified until now is related to various optimizations needed by routing for mobile networks and dedicated hosts within the moving network. One crucial issue in route optimization is the topic of securing the (wide area) route optimization process due to the high potential of possible attacks.